Name: Andrew Hayes
Student ID: 21321503
E-mail: a.hayes18@universityofgalway.ie

CT437

2025-03-21

Assignment 2: Using & Benchmarking Block Ciphers with OpenSSL

1 Block Cipher Benchmarking

Cipher	Key Size (bits)	Mode	Data Size (MB)	Encryption Time (s)	Decryption Time (s)
AES	128	ECB	100	0.011060	0.015951
AES	128	ECB	1000	0.114782	0.138175
AES	128	CBC	100	0.009856	0.013979
AES	128	CBC	1000	0.115273	0.138416
AES	128	CTR	100	0.011900	0.014040
AES	128	CTR	1000	0.127054	0.139111
AES	256	ECB	100	0.009927	0.013479
AES	256	ECB	1000	0.117038	0.138959
AES	256	CBC	100	0.011405	0.014018
AES	256	CBC	1000	0.119599	0.139258
AES	256	CTR	100	0.012812	0.013950
AES	256	CTR	1000	0.114078	0.139007
ARIA	128	ECB	100	0.487708	0.480942
ARIA	128	ECB	1000	4.844433	4.846121
ARIA	128	CBC	100	0.487954	0.484266
ARIA	128	CBC	1000	4.870137	4.865404
ARIA	128	CTR	100	0.484228	0.486427
ARIA	128	CTR	1000	4.864186	4.871898
ARIA	256	ECB	100	0.504303	0.489358
ARIA	256	ECB	1000	5.145704	4.868282
ARIA	256	CBC	100	0.506407	0.538013
ARIA	256	CBC	1000	4.915265	4.887134
ARIA	256	CTR	100	0.506468	0.492493
ARIA	256	CTR	1000	5.093478	5.360305
Camellia	128	ECB	100	0.404620	0.406571
Camellia	128	ECB	1000	4.303221	4.169631
Camellia	128	CBC	100	0.442378	0.418638
Camellia	128	CBC	1000	4.174943	4.098693
Camellia	128	CTR	100	0.416031	0.409108
Camellia	128	CTR	1000	4.116773	4.160921
Camellia	256	ECB	100	0.411045	0.439396
Camellia	256	ECB	1000	4.498530	4.246740
Camellia	256	CBC	100	0.424309	0.421895
Camellia	256	CBC	1000	4.230347	4.341175
Camellia	256	CTR	100	0.413531	0.424235
Camellia	256	CTR	1000	4.198038	4.237361

Table 1: Benchmarking results from TSV file

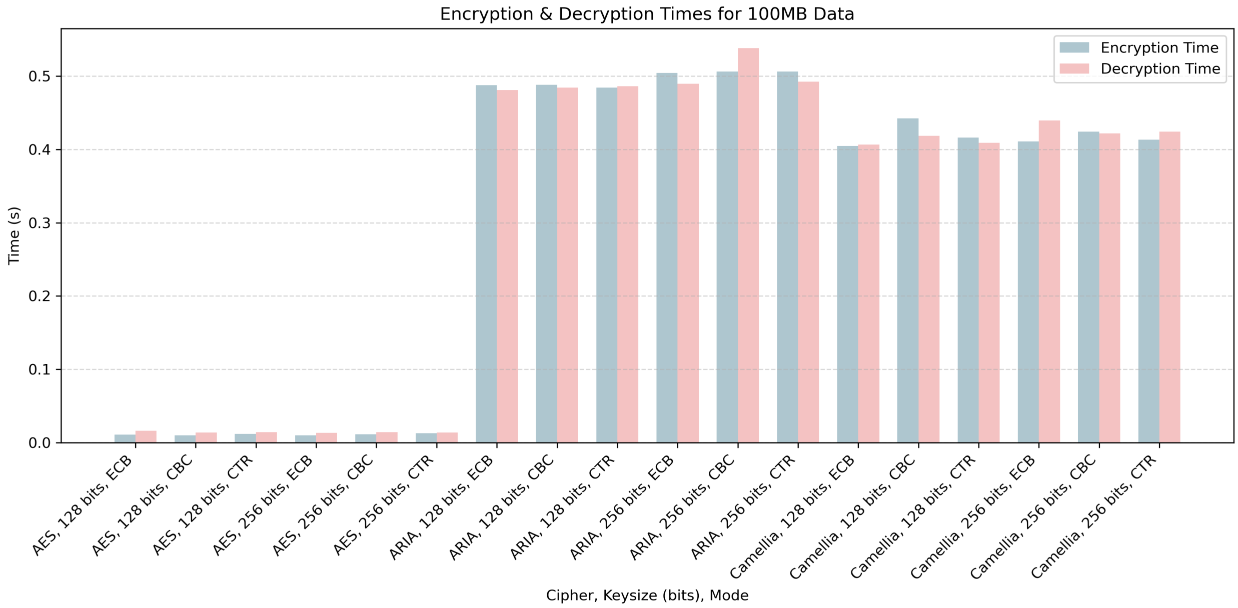

Figure 1: Encryption & decryption times for 100MB data

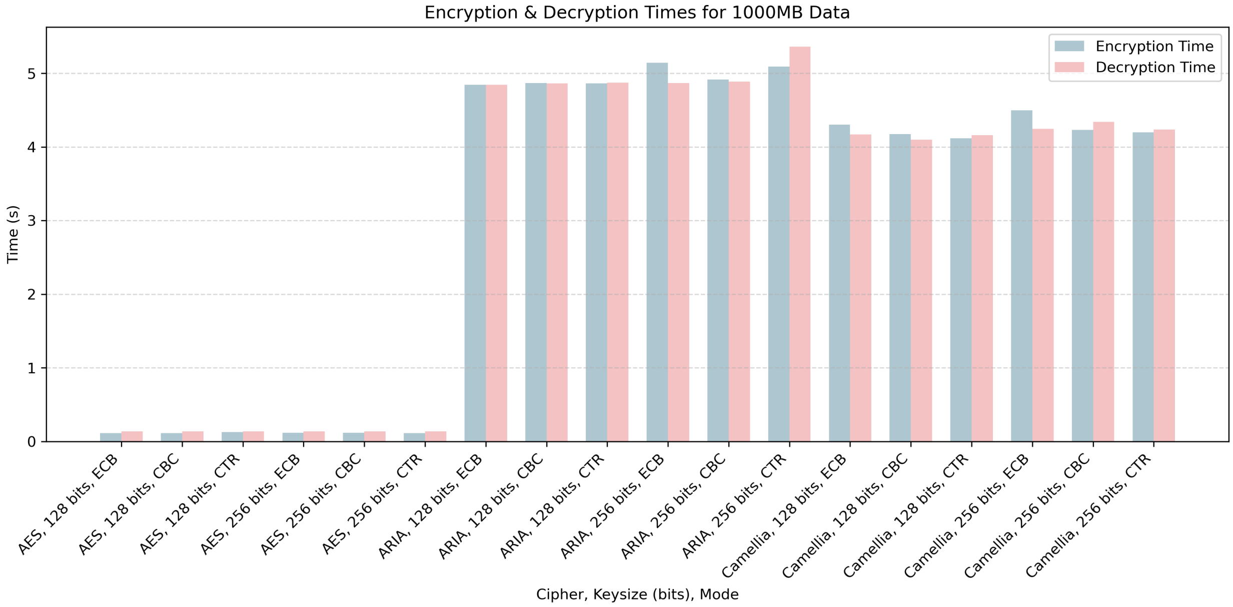

Figure 2: Encryption & decryption times for 1000MB data

2 Implementing & Benchmarking Triple-DES